Následující tvrzení dokládá praktickou použitelnost schématu RSA. V kontextu vyložené látky (pojmy, popis elementárních metod a souvisejících algoritmů – viz snímky promítané při přednáškách) ukazuje na úrovni transformací RSAES (= RSAVP) a RSADP (= RSASP) splnění základního předpokladu k tomu, že každá korektně zašifrovaná zpráva bude správně odšifrována, respektive že každý korektně vytvořený digitální podpis zprávy bude ověřen jako platný. Poznamenejme, že níže uvedený důkaz tohoto tvrzení se svým provedením poněkud odlišuje od běžně uváděných důkazů, které vycházejí z Eulerovy věty ($y^{\phi(n)} \equiv 1 \pmod{n}$, kde $y, n \in \mathbf{Z}$, $n > 1$, $\gcd(y, n) = 1$), ale často neošetřují jeho platnost pro takové zprávy y, jejichž hodnota je soudělná s modulem RSA n. S ohledem na velikost modulu n a jeho faktorů je sice prakticky téměř nemožné, že by se takový případ při obvyklém způsobu používání RSA vyskytl, nicméně pro kryptoanalytické zacházení s RSA je vhodné uvést a dokázat následující tvrzení tak, jak je zde učiněno.

Tvrzení (O schématu RSA). *Buď* (n, e) *veřejný a* (n, d) *privátní klíč RSA. Pak pro* m, $m \in \mathbf{Z}$, *platí*

$m \equiv RSADP(RSAES(m)) \pmod{n}$ *a*

$m \equiv RSAES(RSADP(m)) \pmod{n}$.

Důkaz. Z definice schématu RSA máme $RSAES(y) = y^e \bmod n$ a $RSADP(y) = y^d \bmod n$. Dále víme, že $n = pq$, kde p a q jsou prvočísla, $p,q > 2$, a že veřejný a privátní exponent splňují podmínku $ed \equiv 1 \pmod{\lambda}$, kde $\lambda = \mathrm{lcm}(p - 1, q - 1)$. Označme $x = RSADP(RSAES(m))$, platí $x \equiv m^{ed} \pmod{n}$. Odtud $n|(x - m^{ed})$, speciálně potom $p,q|(x - m^{ed})$.

Nejprve ukážeme, že $p|(x - m)$. Pokud $p|m$, potom také $p|m^{ed}$, takže z výše uvedeného rovněž $p|x$ a uvedený vztah je triviálně splněn. Pokud $\gcd(p, m) = 1$, můžeme použít malou Fermatovu větu. Z vlastností veřejného a privátního klíče RSA plyne $ed = r\lambda + 1$, kde $r \in \mathbf{Z}$. Odtud $x \equiv m^{r\lambda + 1} \equiv m*m^{r\lambda} \pmod{p}$. Protože $(p - 1)|r\lambda$, můžeme s využitím malé Fermatovy věty psát $m^{r\lambda} \equiv 1 \pmod{p}$, takže $x \equiv m \pmod{p}$, odkud $p|(x - m)$.

Analogicky lze ukázat, že také $q|(x - m)$.

Protože $p|(x - m)$ a $q|(x - m)$, tak také $n|(x - m)$, takže $x \equiv m \pmod{n}$.

Dokázali jsme, že $m \equiv RSADP(RSAES(m)) \pmod{n}$, odkud už plyne i platnost $m \equiv RSAES(RSADP(m)) \pmod{n}$, neboť platí $(m^e)^d \equiv (m^d)^e \pmod{n}$.

■

Důsledek. *Buď* (n, e) *veřejný a* (n, d) *privátní klíč RSA. Pak pro celé číslo* m, $0 \le m < n$, *platí*

$m = RSADP(RSAES(m))$ *a*

$m = RSAES(RSADP(m))$.

Důkaz. Důsledek vyplývá z tvrzení o schématu RSA a podmínek $0 \le RSADP(RSAES(m)) < n$, $0 \le RSAES(RSADP(m)) < n$ a $0 \le m < n$.

■

K prokázání korektnosti schématu DSA (opět v kontextu vyložené látky) uvádíme následující tvrzení, které ukazuje, že každý korektně vytvořený digitální podpis zprávy bude na úrovni ověřovacího algoritmu ověřen jako platný.

Tvrzení (O ověření podpisu DSA). *Mějme instanci DSA zadanou veřejnými parametry* (p, q, α)*, privátním klíčem* x *a veřejným klíčem* y*. Dále mějme zprávu* m *a hodnoty* (r, s)*, pro které platí*

$r = (\alpha^k \bmod p) \bmod q$, *kde* $k \in \mathbf{Z}$, $\gcd(k, q) = 1$, $r > 0$,

$s = (h(m) + xr)k^{-1} \bmod q$, *kde* $kk^{-1} \equiv 1 \pmod{q}$ *a* h *je hašovací funkce,* h = SHA-1, $h(m) \in \mathbf{Z}$, $s > 0$.

Potom pro hodnotu v *vypočtenou jako*

$v = (\alpha^c y^d \bmod p) \bmod q$, *kde* $c = h(m)s^{-1} \bmod q$, $d = rs^{-1} \bmod q$, kde $ss^{-1} \equiv 1 \pmod{q}$,

platí $v = r$.

Důkaz. Z definice schématu DSA vyplývá, že řád prvku α v $\mathbf{Z}_p^*$ je roven q, kde q je prvočíslo. Dále platí $y = \alpha^x \bmod p$. Označme $w = \alpha^c y^d \bmod p$, potom $v = w \bmod q$. Z rovnice pro veřejný klíč y dostáváme $w = \alpha^{c+xd} \bmod p$. Dále platí, že $c + xd \equiv h(m)s^{-1} + xrs^{-1} \equiv (h(m) + xr)s^{-1} \equiv k \pmod{q}$. Odtud $c + xd = zq + k$, kde $z \in \mathbf{Z}$, takže $w = \alpha^{zq+k} \bmod p$. Protože $(\alpha^q)^z \equiv 1 \pmod{p}$, můžeme psát $w = \alpha^k \bmod p$. Nyní již snadno ověříme, že pro v platí $v = (\alpha^k \bmod p) \bmod q = r$, QED.

■